# JP10240500

Publication Title:

RANDOM NUMBER GENERATOR AND METHOD, ENCIPHERING DEVICE AND METHOD, DECODER AND METHOD AND STREAM CIPHER SYSTEM

Abstract:

PROBLEM TO BE SOLVED: To obtain a random number generator whose linear complexity is large in comparison with a device scale and which is also cryptographically secure by sequentially changing a 1st random number series that is generated based on a 2nd random number series that is generated.

SOLUTION: This device is provided with a 1st random number generating part 2, a 2nd random number generating part 4 and a random number converting part 6. The part 2 generates random number series (binary series) and outputs it after it is set to an initial state. Similarly, the part 4 generates random number series binary series) and outputs it after it is set to an initial state. The part 6 switches orders of inputted binary series based on binary series that are differently inputted and outputs them. Random number series (a) which are outputted from the part 2 are inputted to the part 6, and the part 6 switches the orders of the random number series (a) which are outputted from the part 2 through the procedure or operation based on random number series (b) which are outputted from the part 4 and outputs them.

---

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－240500

(43)公開日　平成10年(1998)９月11日

| (51)Int.Cl.[6] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 7/58 | | Ｇ０６Ｆ | 7/58 | Ａ |
| | | | | | Ｂ |
| Ｇ０９Ｃ | 1/00 | ６５０ | Ｇ０９Ｃ | 1/00 | ６５０Ｂ |

審査請求　未請求　請求項の数15　ＯＬ　（全 16 頁）

(21)出願番号　特願平9－45954

(22)出願日　平成９年(1997)２月28日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　清水　秀夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　川村　信一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

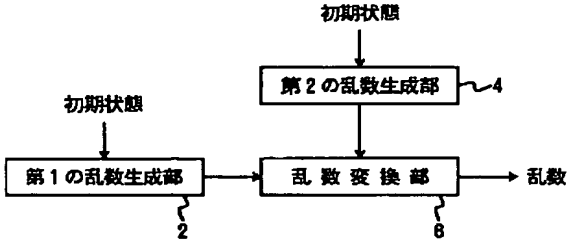
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　乱数生成装置及び方法、暗号化装置及び方法、復号装置及び方法、並びにストリーム暗号システム

(57)【要約】

【課題】　装置規模に比して線形複雑度が大きく暗号的にも安全な乱数生成装置を提供すること。

【解決手段】　所定の初期状態をもとに第１の乱数系列を生成する手段と、所定の初期状態をもとに第２の乱数系列を生成する手段と、第１の乱数系列を、第２の乱数系列に基づいて順序変更する手段を備える。また、所定の初期状態をもとに第１の乱数系列を所定ビット長単位に生成する第１の線形フィードバックシフトレジスタと、所定の初期状態をもとに第２の乱数系列を所定ビット長単位に生成する第２の線形フィードバックシフトレジスタと、第２の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に該アドレスに第１の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する記憶装置を備える。



【特許請求の範囲】
【請求項１】所定の初期状態をもとに第１の乱数系列を生成する第１の乱数生成手段と、
所定の初期状態をもとに第２の乱数系列を生成する第２の乱数生成手段と、
生成された前記第１の乱数系列を、生成された前記第２の乱数系列に基づいて順序変更する変換手段とを備えたことを特徴とする乱数生成装置。
【請求項２】所定の初期状態をもとに第１の乱数系列を所定のビット長単位に生成する第１の線形フィードバックシフトレジスタと、
所定の初期状態をもとに第２の乱数系列を所定のビット長単位に生成する第２の線形フィードバックシフトレジスタと、
前記第２の線形フィードバックシフトレジスタから与えられた前記所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に、該アドレスに前記第１の線形フィードバックシフトレジスタから与えられた前記所定のビット長の乱数を格納する記憶装置とを備えたことを特徴とする乱数生成装置。
【請求項３】所定の初期状態をもとに２値乱数を順次出力する第１の線形フィードバックシフトレジスタと、
所定の初期状態をもとに２値乱数を順次出力する第２の線形フィードバックシフトレジスタと、
前記第２の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に、該アドレスに前記第１の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する第１の記憶装置と、
前記第１の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に、該アドレスに前記第２の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する第２の記憶装置と、
前記第１の記憶装置から出力された所定のビット長の乱数と前記第２の記憶装置から出力された所定のビット長の乱数とを入力とする非線形変換処理を行って所定のビット長の乱数を生成して出力する非線形コンバイナとを備えたことを特徴とする乱数生成装置。
【請求項４】所定の初期状態をもとに生成した第１の乱数系列を、所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して出力することを特徴とする乱数生成方法。
【請求項５】所定の初期状態をもとに第１の乱数系列を生成する第１の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、記憶装置の各アドレスの内容として格納し、
所定の初期状態をもとに第２の乱数系列を生成する第２の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記記憶装置のアドレスに格納されている内容を乱数として出力し、
この内容を出力された前記記憶装置のアドレスに、前記第１の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納し、
以降、前記記憶装置から出力された乱数系列が所定の長さに達するまで、前記記憶装置からの乱数の出力と前記記憶装置への乱数の格納を繰り返し実行することを特徴とする乱数生成方法。
【請求項６】所定の初期状態をもとに第１の乱数系列を生成する第１の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、第１の記憶装置の各アドレスの内容として格納するとともに、所定の初期状態をもとに第２の乱数系列を生成する第２の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、第２の記憶装置の各アドレスの内容として格納し、
前記第２の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記第１の記憶装置のアドレスに格納されている内容を出力して２入力１出力の非線形コンバイナに与えるとともに、前記第１の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記第２の記憶装置のアドレスに格納されている内容を出力して前記非線形コンバイナに与え、この非線形コンバイナにより非線形変換処理を行って所定のビット長の乱数を生成して出力し、
前記第１の記憶装置の前記内容の出力されたアドレスに、前記第１の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納するとともに、前記第２の記憶装置の前記内容の出力されたアドレスに、前記第２の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納し、
以降、前記非線形コンバイナから出力された乱数系列が所定の長さに達するまで、前記第１および第２の記憶装置からの乱数の出力をもとにした非線形変換処理と前記第１および第２の記憶装置への乱数の格納を繰り返し実行することを特徴とする乱数生成方法。
【請求項７】共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、
平文および暗号文の一方の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の２値系列を生成する論理演算手段とを備えたことを特徴とする暗号処理装置。
【請求項８】前記論理演算手段は、ビット単位の排他的論理和演算を行うものであることを特徴とする請求項７

に記載の暗号処理装置。
【請求項９】共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力し、
平文および暗号文の一方の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の２値系列を生成することを特徴とする暗号処理方法。
【請求項１０】共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、
平文の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の２値系列を生成する論理演算手段とを備えたことを特徴とする暗号化装置。
【請求項１１】共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力し、
平文の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の２値系列を生成することを特徴とする暗号化方法。
【請求項１２】共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、
暗号文の２値系列と前記鍵系列とをもとに予め定められた論理演算を行ってもとの平文の２値系列を生成する論理演算手段とを備えたことを特徴とする復号装置。
【請求項１３】共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力し、
暗号文の２値系列と前記鍵系列とをもとに予め定められた論理演算を行ってもとの平文の２値系列を生成することを特徴とする復号方法。
【請求項１４】所定の共通鍵をもとに平文を暗号文に変換する暗号化装置と該所定の共通鍵をもとに暗号文をもとの平文に変換する復号装置と該暗号化装置から該復号装置へ暗号文を伝える所定の媒体とを備えたストリーム暗号システムにおいて、
前記暗号化装置は、
共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、
平文の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の２値系列を生成する論理演算手段とを備え、
前記復号装置は、
共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する、前記乱数生成手段と同一の論理構造を持つ乱数生成手段と、
暗号文の２値系列と前記鍵系列とをもとに前記論理演算と同一の論理演算を行ってもとの平文の２値系列を生成する論理演算手段とを備えたことを特徴とするストリーム暗号システム。
【請求項１５】一方の処理装置にて所定の共通鍵をもとに平文を暗号文に変換し、該暗号文を所定の媒体に出力し、他方の処理装置にて該暗号文を該所定の媒体を通じて入力し、該所定の共通鍵をもとに暗号文をもとの平文に変換するストリーム暗号システムにおいて、
前記処理装置は、
共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、
平文および暗号文の一方の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の２値系列を生成する論理演算手段とを備えたことを特徴とするストリーム暗号システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、簡易な構成でかつ暗号に使用しても安全な乱数生成装置及び方法、その疑似乱数生成器を用いた暗号化装置及び方法、復号装置及び方法、並びにストリーム暗号システムに関する。
【０００２】
【従来の技術】現在、暗号方式として様々なものが知られているが、その１つに加算型ストリーム暗号がある。加算型ストリーム暗号は、良く知られているように、暗号側と復号側で同一または同一の論理構造の疑似乱数生成器を持ち、暗号側では平文メッセージと共通鍵にて示される初期状態にセットされた疑似乱数生成器から出力される乱数系列（鍵系列）とをビット単位に足し込む（排他的論理和が良く用いられる）ことで暗号化を行い、復号側ではこの暗号化されたメッセージを入力として暗号側と同一の手順を実行することにより復号化を行うものである。
【０００３】このような加算型ストリーム暗号のなかでも、M系列を出力する線形フィードバックシフトレジスタを疑似乱数生成器として利用する構成は、装置規模が小さくなることもあり、良く用いられている。図１３に線形フィードバックシフトレジスタの原理図を示す。図中の$C_1$～$C_n$は予め０または１に定められ、ｎ段のシ

フトレジスタ$S_{i-k}$の値のうち$C_k$＝１であるものの排他的論理和が出力$S_i$になり、シフト動作においてこの$S_i$がフィードバックされる。また、線形フィードバックシフトレジスタをセットする初期状態が共通鍵となる。

【０００４】しかしながら、線形フィードバックシフトレジスタ自体は、レジスタ長の２倍の出力を観測することで、その構造と初期状態のすべてを特定することが可能なので、加算型ストリーム暗号に用いる疑似乱数生成器としては、安全性に関して問題がある。また、線形フィードバックレジスタを疑似乱数生成器として用いるために、レジスタ長を長くして安全性を高めようとすることは、装置規模の点から問題がある。

【０００５】そこで、複数の線形フィードバックシフトレジスタの出力を非線形コンバイナで結合する手法や、線形フィードバックシフトレジスタの出力に非線形変換を施す手法等が開発されている（例えば文献１「暗号理論入門」、共立出版株式会社、岡本栄司著、１９９３年発行などに詳しい）。

【０００６】しかし、複数の線形フィードバックシフトレジスタの出力を非線形コンバイナで結合する方式では、線形複雑度はたかだか各線形フィードバックシフトレジスタのレジスタ長の積程度にしかならない。

【０００７】ここで、線形複雑度は、疑似乱数生成器の解読しずらさ、すなわち暗号学的な安全性を計るための尺度として用いられる指標で、「ある初期値から始めれば同じ出力と同じ周期をもつという意味で等価な線形フィードバックシフトレジスタのレジスタ長」と定義される（文献１参照）。

【０００８】そこで、装置規模に比して線形複雑度が大きくなる疑似乱数生成器があれば、経済的にも安全性の観点からも非常に都合が良い。そのような疑似乱数生成器の候補として、加算ジェネレータ（ｓｕｍｍａｔｉｏｎ ｇｅｎｅｒａｔｏｒ；例えば文献２“ＡＰＰＬＩＤＥ ＣＲＹＰＴＯＧＲＡＰＨＹ”、Ｊｏｈｎ Ｗｉｌｅｙ ＆ Ｓｏｎｓ，Ｉｎｃ．社、１９９６年発行、ｐｐ．３８６～３８７に詳しい）が提案された。図１４に加算ジェネレータの一例を示す。この場合、シフトレジスタ$b_1$と$b_2$とキャリアの和を２で割った剰余をシフトレジスタにフィードバックするとともに、$b_1$と$b_2$とキャリアの和を２で割った商を新たなキャリアとして保持する動作を繰り返す。

【０００９】ところが、加算ジェネレータの線形複雑度は線形フィードバックシフトレジスタのレジスタ長の指数程度となることが知られているが、加算ジェネレータは既に解読されており、加算型ストリーム暗号に用いる疑似乱数生成器としては、安全性に関して問題がある。

【００１０】

【発明が解決しようとする課題】以上説明したように、従来、小さな装置規模で安全性の高いストリーム暗号を実現し得る線形複雑度の大きな乱数生成装置は知られていなかった。本発明は、上記事情を考慮してなされたもので、装置規模に比して線形複雑度が大きく暗号的にも安全な乱数生成装置及び方法、暗号化装置及び方法、復号装置及び方法、並びにストリーム暗号システムを提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明（請求項１）に係る乱数生成装置は、所定の初期状態をもとに第１の乱数系列を生成する第１の乱数生成手段と、所定の初期状態をもとに第２の乱数系列を生成する第２の乱数生成手段と、生成された前記第１の乱数系列を、生成された前記第２の乱数系列に基づいて順序変更する変換手段とを備えたことを特徴とする。

【００１２】本発明（請求項２）に係る乱数生成装置は、所定の初期状態をもとに第１の乱数系列を所定のビット長単位に生成する第１の線形フィードバックシフトレジスタと、所定の初期状態をもとに第２の乱数系列を所定のビット長単位に生成する第２の線形フィードバックシフトレジスタと、前記第２の線形フィードバックシフトレジスタから与えられた前記所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に、該アドレスに前記第１の線形フィードバックシフトレジスタから与えられた前記所定のビット長の乱数を格納する記憶装置とを備えたことを特徴とする。

【００１３】なお、１つの線形フィードバックシフトレジスタのみ設け、これを第１の線形フィードバックシフトレジスタおよび第２の線形フィードバックシフトレジスタとして用いても良い。

【００１４】また、一部または全部の線形フィードバックシフトレジスタを、他の公知の乱数生成器に置き換えても良い。本発明（請求項３）に係る乱数生成装置は、所定の初期状態をもとに２値乱数を順次出力する第１の線形フィードバックシフトレジスタと、所定の初期状態をもとに２値乱数を順次出力する第２の線形フィードバックシフトレジスタと、前記第２の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に、該アドレスに前記第１の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する第１の記憶装置と、前記第１の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に、該アドレスに前記第２の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する第２の記憶装置と、前記第１の記憶装置から出力された所定のビット長の乱数と前記第２の記憶装置から出力された所定のビット長の乱数とを入力とする非線形変換処理を行って所定のビット長の乱数を生成して出力する非線形コンバイナとを備えたことを特徴とする。

【００１５】なお、第１の線形フィードバックシフトレジスタを記憶装置に格納するデータ用と記憶装置に与えるアドレス用で共用する代わりに、データ専用とアドレス専用の２つの線形フィードバックシフトレジスタを設けても良い。同様に、第２の線形フィードバックシフトレジスタも共用する代わりに、データ専用とアドレス専用の２つの線形フィードバックシフトレジスタを設けても良い。

【００１６】また、一部または全部の線形フィードバックシフトレジスタを、他の公知の乱数生成器に置き換えても良い。本発明に係る乱数生成装置における一部または全部の線形フィードバックシフトレジスタを、本発明に係る乱数生成装置自体で置き換えても良い。この置き換えは、何階層に渡って行っても良い。

【００１７】本発明（請求項４）に係る乱数生成方法は、所定の初期状態をもとに生成した第１の乱数系列を、所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して出力することを特徴とする。

【００１８】本発明（請求項５）に係る乱数生成方法は、所定の初期状態をもとに第１の乱数系列を生成する第１の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、記憶装置の各アドレスの内容として格納し、所定の初期状態をもとに第２の乱数系列を生成する第２の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記記憶装置のアドレスに格納されている内容を乱数として出力し、この内容を出力された前記記憶装置のアドレスに、前記第１の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納し、以降、前記記憶装置から出力された乱数系列が所定の長さに達するまで、前記記憶装置からの乱数の出力と前記記憶装置への乱数の格納を繰り返し実行することを特徴とする。

【００１９】本発明（請求項６）に係る乱数生成方法は、所定の初期状態をもとに第１の乱数系列を生成する第１の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、第１の記憶装置の各アドレスの内容として格納するとともに、所定の初期状態をもとに第２の乱数系列を生成する第２の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、第２の記憶装置の各アドレスの内容として格納し、前記第２の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記第１の記憶装置のアドレスに格納されている内容を出力して２入力１出力の非線形コンバイナに与えるとともに、前記第１の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記第２の記憶装置のアドレスに格納されている内容を出力して前記非線形コンバイナに与え、この非線形コンバイナにより非線形変換処理を行って所定のビット長の乱数を生成して出力し、前記第１の記憶装置の前記内容の出力されたアドレスに、前記第１の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納するとともに、前記第２の記憶装置の前記内容の出力されたアドレスに、前記第２の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納し、以降、前記非線形コンバイナから出力された乱数系列が所定の長さに達するまで、前記第１および第２の記憶装置からの乱数の出力をもとにした非線形変換処理と前記第１および第２の記憶装置への乱数の格納を繰り返し実行することを特徴とする。

【００２０】本発明（請求項７）に係る暗号処理装置は、共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、平文および暗号文の一方の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の２値系列を生成する論理演算手段とを備えたことを特徴とする。

【００２１】本発明（請求項９）に係る暗号処理方法は、共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力し、平文および暗号文の一方の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の２値系列を生成することを特徴とする。

【００２２】本発明（請求項１０）に係る暗号化装置は、共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、平文の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の２値系列を生成する論理演算手段とを備えたことを特徴とする。

【００２３】本発明（請求項１１）に係る暗号化方法は、共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力し、平文の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の２値系列を生成することを特徴とする。

【００２４】本発明（請求項１２）に係る復号装置は、共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、暗号文の２値系列と前記鍵系列とをもとに予め定められた論

理演算を行ってもとの平文の２値系列を生成する論理演算手段とを備えたことを特徴とする。

【００２５】本発明（請求項１３）に係る復号方法は、共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力し、暗号文の２値系列と前記鍵系列とをもとに予め定められた論理演算を行ってもとの平文の２値系列を生成することを特徴とする。

【００２６】本発明（請求項１４）は、所定の共通鍵をもとに平文を暗号文に変換する暗号化装置と該所定の共通鍵をもとに暗号文をもとの平文に変換する復号装置と該暗号化装置から該復号装置へ暗号文を伝える所定の媒体とを備えたストリーム暗号システムにおいて、前記暗号化装置は、共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、平文の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の２値系列を生成する論理演算手段とを備え、前記復号装置は、共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する、前記乱数生成手段と同一の論理構造を持つ乱数生成手段と、暗号文の２値系列と前記鍵系列とをもとに前記論理演算と同一の論理演算を行ってもとの平文の２値系列を生成する論理演算手段とを備えたことを特徴とする。

【００２７】本発明（請求項１５）は、一方の処理装置にて所定の共通鍵をもとに平文を暗号文に変換し、該暗号文を所定の媒体に出力し、他方の処理装置にて該暗号文を該所定の媒体を通じて入力し、該所定の共通鍵をもとに暗号文をもとの平文に変換するストリーム暗号システムにおいて、前記処理装置は、共通鍵により与えられる所定の初期状態をもとに生成した第１の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第２の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、平文および暗号文の一方の２値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の２値系列を生成する論理演算手段とを備えたことを特徴とする。

【００２８】本発明における論理演算は、例えば、ビット単位の排他的論理和演算である。なお、本発明の暗号処理、暗号装置、復号装置の乱数生成手段には、請求項２の乱数生成装置や請求項３の乱数生成装置や上述したようにこれらを変形したものを適用することもできる。

【００２９】本発明では、記憶装置を緩衝域として用い、第１の線形フィードバックシフトレジスタＡの出力を該記憶装置のアドレスとして入力し、該アドレスに記憶されている内容を乱数として出力し、該アドレスに第２の線形フィードバックシフトレジスタＢの出力をデータ入力として記憶することで、線形複雑度の大きな乱数生成装置を実現することができる。

【００３０】線形フィードバックシフトレジスタＡとＢのレジスタ長を各々ＬＡ，ＬＢとする。請求項２等に係る発明のように記憶装置を緩衝域として用いる乱数生成装置での線形複雑度は、ほぼＬＡ×$2^{LB}$である。

【００３１】請求項３等に係る発明の２つの記憶装置を互いの緩衝域として用いる乱数生成器での線形複雑度は、ほぼ$2^{LA}\times 2^{LB}$である。また、乱数生成装置を用いるストリーム暗号では、暗号の解読しずらさという意味での安全性を計るための尺度として、線形複雑度が用いられる。つまり、線形装置規模に比して線形複雑度が大きいことは、安価に安全な暗号装置を構築できることを意味する。

【００３２】このように本発明によれば、少ない装置規模で大きな線形複雑度を達成できるので、経済的に安全な暗号を実現できる。なお、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【００３３】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。本発明に係る乱数生成装置および方法は、装置規模に比して大きな線形複雑度を得ることができるものであり、もちろん乱数を必要とする種々の分野に適用可能であるが、特に、統計的性質だけでなく予測可能性、端的に言えばアタックに対する安全性をも問題とされる暗号、中でもストリーム暗号に好適なものである。

【００３４】最初に、本発明の乱数生成装置および方法の基本的な考え方について説明する。図１に、本発明の一実施形態に係る乱数生成装置の構成を示す。

【００３５】本乱数生成装置は、第１の乱数生成部２と、第２の乱数生成部４と、乱数変換部６を備えている。第１の乱数生成部２は、初期状態にセットされた後、乱数系列（２値系列）ａを生成し出力していく。

【００３６】同様に、第２の乱数生成部４は、初期状態にセットされた後、乱数系列（２値系列）ｂを生成し出力していく。なお、第１の乱数生成部２は、初期状態が同一であれば、同一の乱数系列を生成する。第２の乱数生成部４についても同様である。また、第１の乱数生成部２や第２の乱数生成部４についての初期状態とは、例えば内部変数あるいは各レジスタの保持する値の初期値群であり、例えば線形フィードバックシフトレジスタにおける各シフトレジスタの保持する初期値の組がこれに該当する。

【００３７】また、第１の乱数生成部２の初期状態と第２の乱数生成部４の初期状態は独立のものであるが、第

１の乱数生成部２と第２の乱数生成部４が同様の構成の場合に同一のものを使用しても構わない。

【００３８】乱数変換部６は、入力された２値系列の順序を、別に入力された２値系列に基づいて入れ替えて出力する。また、２値系列の順序の入れ替えは、連続する所定のビット数（１ビットの場合を含む）を一纏まりとして行われる。

【００３９】入れ替えの方法は、乱数変換部６は、入力された２値系列ａの順序を、別に入力された２値系列ｂに基づいて入れ替えて出力する。２値系列ａの順序の入れ替えは、連続する所定のビット数（１ビットの場合を含む）を一纏まりとして行われる。例えば、連続する６４ビットを一纏まりとする。

【００４０】２値系列ａの順序の入れ替えの方法は、例えば、上記の別に入力された２値系列ｂを連続するｎビット（例えば８ビット）ごとに区切って得た２進数ｎビットの情報の系列に従って、２値系列ａ中のある位置の一纏まりを他の位置（結果的に同じ位置になる場合を含む）に移す。

【００４１】２値系列ａが同一でも、２値系列ｂが相違すれば、乱数変換部６の出力として得られる乱数系列は相違するものとなる。また、第１の乱数生成部２の初期状態と第２の乱数生成部４の初期状態の組が同一であれば、乱数変換部６の出力として得られる乱数系列は同一になる。

【００４２】詳しくは後述するが、この乱数変換部６は、例えばＲＡＭなどの記憶装置を用いることにより実現することが可能である。図１において、第１の乱数生成部２から出力された乱数系列ａが乱数変換部６に入力され、乱数変換部６では第２の乱数生成部４から出力された乱数系列ｂに基づいた手順または動作で、第１の乱数生成部２から出力された乱数系列ａの順序を入れ替えて出力する。

【００４３】例えば、乱数系列ａが$a_1$，$a_2$，$a_3$，$a_4$，$a_5$，$a_6$，$a_7$，$a_8$，…（$a_i$は０または１）で、乱数変換部６は連続する２ビットを一纏まりとして順序の入れ替えを行う場合、乱数変換部６から出力される乱数系列は、乱数系列ｂの内容に応じて、$a_3$，$a_4$，$a_7$，$a_8$，$a_1$，$a_2$，…、あるいは$a_5$，$a_6$，$a_1$，$a_2$，$a_7$，$a_8$，…などとなる。

【００４４】なお、図１の乱数生成装置の他の例として、第１の乱数生成部２と第２の乱数生成部４とを１つに共通化しても良い。この場合、第１の乱数生成部２として所定のビット数の乱数を生成する動作と、第２の乱数生成部４として所定のビット数の乱数を生成する動作とを交互に行えば良い。言い換えると、この共通化された乱数生成装置から出力される乱数系列を、上記の２値系列ａ用と２値系列ｂ用に交互に使えば良い。

【００４５】また、図１の乱数生成装置のさらに他の例として、図１の乱数生成装置における第１の乱数生成部２および第２の乱数生成部４の少なくとも一方を、図１の乱数生成装置自体で置き換えた構成にしても良い。

【００４６】次に、本発明の乱数生成装置をストリーム暗号に適用する場合について説明する。ストリーム暗号では、暗号側において、平文メッセージ（２値系列）と所定の共通鍵に基づいて生成された鍵系列（２値系列）にビット単位の所定の論理演算（一般的には排他的論理和演算）を施して暗号文を生成し、復号側において、暗号文（２値系列）と所定の共通鍵（暗号側で使用した鍵と同一のもの）に基づいて生成された暗号側と同一の鍵系列にビット単位の所定の論理演算（暗号側で使用した演算と同一のもの）を施してもとの平文メッセージを得る。

【００４７】このようなストリーム暗号において、上記の鍵系列を生成する装置として、前述したまたは後述する本実施形態の乱数生成装置を用いると効果的である。この場合、乱数生成装置の初期状態は、共通鍵として与えられるようにする。

【００４８】図２に、本発明の乱数生成装置をストリーム暗号に適用した暗号システムの構成例を示す。暗号側（例えばデータを伝える媒体に通信路を用いる場合の送信側）の暗号装置には、本実施形態の乱数生成装置１０ａと、論理演算処理装置１２ａが備えられている。

【００４９】同様に、復号側（例えばデータを伝える媒体に通信路を用いる場合の受信側）の復号装置には、本実施形態の乱数生成装置１０ｂと、論理演算処理装置１２ｂが備えられている。

【００５０】乱数生成装置１０ａと乱数生成装置１０ｂとは同一または同一の論理構造を持つものであり、論理演算処理装置１２ａと論理演算処理装置１２ｂとは同一または等価なものである。なお、ここでは、論理演算処理装置１２ａと論理演算処理装置１２ｂは、ビット単位の排他的論理和演算を行うものとして説明する。

【００５１】図２において、暗号側と復号側との間では、何らかの公知の方法で共通鍵を共有しているものとする。この共通鍵により、乱数生成装置１０ａおよび１１の初期状態が与えられる。共通鍵の内容は、乱数生成装置１０ａおよび１１の初期状態そのものであっても良いし、初期状態を特定可能な識別子でも良い。

【００５２】そして、暗号側では、暗号化したい平文メッセージと、所定の共通鍵により与えられる初期状態をもとにした乱数生成装置１０ａの生成する乱数系列との排他的論理和を取って、平文メッセージを暗号文に変換し、通信路等を介して暗号側に伝える。

【００５３】暗号文を取得した復号側では、この暗号文と、前記共通鍵により与えられる初期状態をもとにした乱数生成器１０ｂの生成する乱数系列との排他的論理和を取ることにより、もとの平文メッセージを復元する。

【００５４】たとえ不正な盗聴者がたとえ暗号文を入手したとしても、共通鍵を知らないので、平文を復元する

ことはできない。なお、暗号側から復号側に暗号文を渡すための手段はどのようなものであっても構わない。例えば、両者をネットワークで接続する方法、無線通信により暗号文を伝送する方法、暗号文を可搬できる記憶媒体に格納して受け渡す方法など種々のものが考えられる。なお、これらに対応する機能部分は、図２においては省略されている。

【００５５】また、暗号装置と復号装置で行う処理は実質的に同じであるので、実際には、計算機などの処理装置は、暗号装置と復号装置の両方の機能を持つことができる。

【００５６】以下では、本発明の実施の形態に係る乱数生成装置についてより詳しく説明していく。図３に、本発明の一実施形態に係る乱数生成装置の構成を示す。また、図４に、本乱数生成装置の動作の流れを示す。

【００５７】本乱数生成装置は、第１の線形フィードバックシフトレジスタ２０、第２の線形フィードバックシフトレジスタ２２、記憶装置２４を備えている。第１の線形フィードバックシフトレジスタ２０および第２の線形フィードバックシフトレジスタ２２夫々の内部基本構成は、既に説明した図１３と同様のものを用いることができる。

【００５８】第１の線形フィードバックシフトレジスタ２０と第２の線形フィードバックシフトレジスタ２２のシフトレジスタ数は、独立に設定することができる。同数でも良いし、異なる数でも良い。また、シフトレジスタ数が同数である場合に、第１の線形フィードバックシフトレジスタ２０と第２の線形フィードバックシフトレジスタ２２の内部構造は、独立に設定することができ、同一構造でも異なる構造でも良い。

【００５９】なお、線形フィードバックシフトレジスタ２０，２２夫々の生成多項式は最大長系列を出力させるために既約多項式であることが望ましい。また、第１の乱数生成部２にセットする初期状態と第２の乱数生成部４にセットする初期状態は独立のものであるが、第１の線形フィードバックシフトレジスタ２０と第２の線形フィードバックシフトレジスタ２２のシフトレジスタ数が同一の場合に、両者の初期状態を同一にしても構わない。

【００６０】上記のような第１の線形フィードバックシフトレジスタ２０は、初期状態にセットされた後、乱数系列（２値系列）Ｄを所定のビット単位（例えば６４ビット単位）に生成し出力していく。この単位となるビット数をｕ１で表す。

【００６１】同様に、第２の乱数生成部４は、初期状態にセットされた後、乱数系列（２値系列）Ａを所定のビット単位（例えば８ビット単位）に生成し出力していく。この単位となるビット数をｕ２で表す。

【００６２】記憶装置２４は、例えばＲＡＭなどのように指定したアドレスに対する書き込みおよび読み出しが可能な記憶素子を用いて構成される。記憶装置２４は、少なくとも$2^{u2}$（＝ｍ）種類のアドレスの夫々にｕ１ビットのデータを格納できる容量を持つものとする。ただし、記憶装置２４は、１つの記憶素子から構成されていても複数の記憶素子から構成されていても構わない。

【００６３】第１の線形フィードバックシフトレジスタ２０から逐次出力されるｕ１ビットの乱数は、記憶装置２４にデータ入力として与えられる。一方、第２の線形フィードバックシフトレジスタ２２から逐次出力されるｕ２ビットの乱数は、記憶装置２４にアドレス入力として与えられる。

【００６４】なお、第２の線形フィードバックシフトレジスタ２２から出力されるｕ２ビットの乱数が直接、記憶装置２４のアドレスを示すものとしても良いし、間接的に、該乱数により記憶装置２４のアドレスが特定されるようにしても良い。例えば、ｕ２＝４で乱数が“１００１”の場合に記憶装置２４のアドレス“１００１”が示されるようにしても良いし、例えば定数＋乱数×４などのアドレス変換式あるいは予め設定されたアドレス変換テーブルにより実際のアドレスが示されるものとしても良い。

【００６５】なお、第２の線形フィードバックシフトレジスタ２２から出力されるｕ２ビットの乱数により、間接的に記憶装置２４のアドレスが特定されるようにする場合における、乱数をアドレスに変換する機能部分については図示を省略した。

【００６６】次に、図４を参照しながら本乱数生成装置の動作について説明する。まず、初期処理として、第１の線形フィードバックシフトレジスタ２０および第２の線形フィードバックシフトレジスタ２２夫々を所望の初期状態にセットする（ステップＳ１）。

【００６７】そして、第１の線形フィードバックシフトレジスタ２０によりｕ１ビットの乱数をｍ個生成し、これらを記憶装置２４のｍ種類のアドレス（例えば０～ｍ－１番地）に夫々格納する（ステップＳ２）。

【００６８】ｍ個の乱数夫々をどのアドレスに格納するかは種々の方法が考えられるが、例えば、生成された順番に０番地～ｍ－１番地へと格納していく。次に、第２の線形フィードバックシフトレジスタ２２によりｕ２ビットの乱数を１つ生成する（ステップＳ３）。

【００６９】そして、記憶装置２４のアドレスのうち、ステップＳ３で生成された乱数にて示されるアドレスの内容（ｕ１ビットの２値データ）を出力する（ステップＳ４）。

【００７０】この時点で、生成すべき乱数系列のうち最初のｕ１ビットのデータが得られたことになる。次に、第１の線形フィードバックシフトレジスタ２０によりｕ１ビットの乱数を１つ生成する（ステップＳ６）。

【００７１】そして、記憶装置２４のアドレスのうち、ステップＳ４で内容の出力されたアドレスに、ステップ

Ｓ５で生成された乱数を格納する（ステップＳ７）。次に、ステップＳ３に戻って第２の線形フィードバックシフトレジスタ２２によりｕ２ビットの乱数を１つ生成する（ステップＳ３）。

【００７２】そして、記憶装置２４のアドレスのうち、ステップＳ３で生成された乱数にて示されるアドレスの内容（ｕ１ビットの２値データ）を出力する（ステップＳ４）。

【００７３】この時点で、生成すべき乱数系列のうち２番目のｕ１ビットのデータが得られたことになり、乱数系列としては全部でｕ１×２ビットのデータが得られたことになる。

【００７４】以降、ステップＳ６，Ｓ７，Ｓ３，Ｓ４の処理ループを１回繰り返すごとに、順次、ｕ１ビットの乱数が生成されていく。そして、ステップＳ４で必要な長さの乱数系列が得られた場合に、ステップＳ５でループを抜けて、処理を終了する。

【００７５】以上により、第１の線形フィードバックシフトレジスタ２０により生成された乱数系列を、第２の線形フィードバックシフトレジスタ２２により生成された乱数系列に基づいて順序変更したものが得られる。

【００７６】以下では、本乱数生成装置の動作について具体例を用いて説明する。ここでは、ｕ２＝３とし、第２の線形フィードバックシフトレジスタ２０により生成された乱数が直接、記憶装置２４のアドレスを示すものとする。

【００７７】また、第１の線形フィードバックシフトレジスタ２０により、乱数系列“ＡＢＣＤＥＦＧＨＩＪＫＬＭＮ…”が生成され、第２の線形フィードバックシフトレジスタ２２により、乱数系列“０１１００１０１１１１０００００１０…”が生成されるものとする。

【００７８】ここで、Ａ～Ｎの各々は、２値の乱数系列を先頭からｕ１ビット毎に区切って得たデータを表すものとする。ｕ２＝３とするので、図５に示すように第２の線形フィードバックシフトレジスタ２０により生成された乱数系列を３ビットごとに区切って得られる“０１１”、“００１”、“０１１”、“１１１”、“０００”、“０１０”、…が、この順番に記憶装置２４にアドレス入力として与えられることになる。

【００７９】動作前においては図６（ａ）のように記憶装置２４のアドレス０００～１１１には有効なデータが格納されていない状態である。まず、$m=2^{u2}=2^3=8$であるので、ステップＳ１において初期状態がセットされた後、ステップＳ２において、第１の線形フィードバックシフトレジスタ２０により、乱数系列“ＡＢＣＤＥＦＧＨ”が生成され、図６（ｂ）のように記憶装置２４のアドレス０００～１１１にされる。

【００８０】次に、ステップＳ３にて第２の線形フィードバックシフトレジスタ２２により“０１１”が生成され、ステップＳ４にて記憶装置２４のアドレス“０１１”の内容Ｄが出力される。

【００８１】そして、ステップＳ６にて第１の線形フィードバックシフトレジスタ２０により“Ｉ”が生成され、これがステップＳ７にて記憶装置２４のアドレス“０１１”に格納される。このときの記憶装置２４の各アドレスの内容を図６（ｃ）に示す。

【００８２】次に、ステップＳ３に戻り、第２の線形フィードバックシフトレジスタ２２により“００１”が生成され、ステップＳ４にて記憶装置２４のアドレス“００１”の内容Ｂが出力される。

【００８３】そして、ステップＳ６にて第１の線形フィードバックシフトレジスタ２０により“Ｊ”が生成され、これがステップＳ７にて記憶装置２４のアドレス“００１”に格納される。このときの記憶装置２４の各アドレスの内容を図６（ｄ）に示す。

【００８４】さらに同様の処理を４回繰り返すと、乱数系列“ＤＢＩＨＡＣ”が得られる。この間の記憶装置２４の各アドレスの内容の遷移を図７（ａ）～（ｄ）に示す。

【００８５】以上の処理を必要回数繰り返すことにより、所望の長さの乱数系列を得ることができる。ここで、図８（ａ）と（ｂ）に、第１の線形フィードバックシフトレジスタ２０により生成された乱数系列と、本乱数生成装置により生成された乱数系列を対象する形で示す。

【００８６】図８に示されるように、第２の線形フィードバックシフトレジスタ２２により生成された乱数系列に基づいて、第１の線形フィードバックシフトレジスタ２０により生成された乱数系列が、ｕ１ビット単位で順序変更されて、本乱数生成装置から出力されていることがわかる。

【００８７】なお、本乱数生成装置は、図２を用いて説明した暗号装置および復号装置における乱数系列（鍵系列）を生成するための乱数生成装置として用いると効果的である。この場合、線形フィードバックシフトレジスタ２０の初期状態および線形フィードバックシフトレジスタ２２の初期状態の組そのものまたはこれらを特定可能な識別子が共通鍵として用いられる。

【００８８】このような本実施形態によれば、記憶装置を緩衝域として用いることで、装置規模に比して線形複雑度が大きく、暗号的にも安全な乱数生成装置、あるいはこれを有する加算型ストリーム暗号の暗号装置および復号装置を実現することができる。

【００８９】また、装置規模に比して線形複雑度が大きいことは、安価に安全な暗号装置および復号装置を構築できることを意味する。ここで、本実施形態の第１および第２の線形フィードバックシフトレジスタのレジスタ長を各々ＬＡ，ＬＢとすると、本乱数生成装置での線形複雑度は、ほぼ

$LA\times 2^{LB}$

である。

【００９０】なお、乱数生成装置の他の構成例として、第１の線形フィードバックシフトレジスタ２０および第２の線形フィードバックシフトレジスタ２２の少なくとも一方を、他の公知の乱数生成装置（例えば、複数の線形フィードバックシフトレジスタの出力を非線形コンバイナで結合するもの、線形フィードバックシフトレジスタの出力に非線形変換を施すもの、あるいは加算ジェネレータ（ｓｕｍｍａｔｉｏｎ　ｇｅｎｅｒａｔｏｒ）など）に置き換えた構成も考えられる。これを図２の暗号装置および復号装置に適用する場合にも、もちろん、置き換えた乱数生成装置の初期状態そのものまたはこれを特定可能な識別子が共通鍵として用いられる。

【００９１】また、図９に示すように、乱数生成装置のさらに他の構成例として、第１の線形フィードバックシフトレジスタ２０と第２の線形フィードバックシフトレジスタ２２とを１つの線形フィードバックシフトレジスタ２６として共通化しても良い。この場合、第１の線形フィードバックシフトレジスタ２０としてｕ１ビットの乱数を生成する動作と、第２の線形フィードバックシフトレジスタ２２としてｕ２ビットの乱数を生成する動作とを交互に行えば良い。さらに、この場合においても、線形フィードバックシフトレジスタ２６を、他の公知の乱数生成装置に置き換えた構成も考えられる。

【００９２】また、線形フィードバックシフトレジスタから出力される乱数系列を単に並べ変えるだけであれば、例えば、線形フィードバックシフトレジスタから出力される乱数系列を適当な長さにきって、一旦バッファ装置に蓄積し、この適当な長さの乱数系列をランダムに並べ変えて出力する方法も考えられるが、この場合、線形フィードバックシフトレジスタでの乱数生成と順番のバッファ装置における並べ変えから出力までの各処理がバッチ的に行われるので、遅延が生じる欠点がある。これに対して、本実施形態によれば、線形フィードバックシフトレジスタでの乱数生成とバッファ装置からの出力が短いサイクルで繰り返し行われるので、遅延が生じないという効果を得ることもできる。

【００９３】図１０に、本発明の他の実施形態に係る乱数生成装置の構成を示す。また、図１１に、本乱数生成装置の動作の流れを示す。本乱数生成装置は、第１の線形フィードバックシフトレジスタ３０、第２の線形フィードバックシフトレジスタ３２、第１の記憶装置３４、第１の記憶装置３６、非線形コンバイナ３８を備えている。

【００９４】本乱数生成装置は、先の実施形態で図３を参照しながら説明した乱数生成装置を２組用意し、それらから得られる２つの乱数系列に非線形変換処理を施したものを出力するものに相当する。ただし、図１０では、線形フィードバックシフトレジスタを各機能専用に４個すべて設けず、併用することで２個だけ設けたものとなっている。

【００９５】すなわち、第１の線形フィードバックシフトレジスタ３０および第２の線形フィードバックシフトレジスタ３２の基本的な構成は、先の実施形態で図３を参照しながら説明した第１の線形フィードバックシフトレジスタ２０および第２の線形フィードバックシフトレジスタ２２と同様である。相違するのは、第１の線形フィードバックシフトレジスタ３０を第１の記憶装置３４へのデータ入力と第２の記憶装置３６へのアドレス入力の両方に使用し、第２の線形フィードバックシフトレジスタ３２を第２の記憶装置３６へのデータ入力と第１の記憶装置３４へのアドレス入力の両方に使用する点である。

【００９６】本実施形態では、第１の線形フィードバックシフトレジスタ３０により生成され第１の記憶装置３４へのデータ入力となる乱数Ｄ１と、第２の線形フィードバックシフトレジスタ３２により生成され第２の記憶装置３６へのデータ入力となる乱数Ｄ２とは、同じビット長でも良いし、異なるビット長でも良い。

【００９７】また、第１の線形フィードバックシフトレジスタ３０により生成され第２の記憶装置３６へのアドレス入力となる乱数Ａ１と、第２の線形フィードバックシフトレジスタ３２により生成され第１の記憶装置３４へのアドレス入力となる乱数Ａ２とは、同じビット長でも良いし、異なるビット長でも良い。

【００９８】ようするに、本実施形態では、第１の線形フィードバックシフトレジスタ３０は、初期処理のために第１の記憶装置３４に格納すべき必要個数の乱数を生成した後は、第２の記憶装置３６へのアドレス入力となる乱数Ａ１と、第１の記憶装置３４へのデータ入力となる乱数Ｄ１とを交互に生成し、同様に、第２の線形フィードバックシフトレジスタ３２は、初期処理のために第２の記憶装置３６に格納すべき必要個数の乱数を生成した後は、第１の記憶装置３４へのアドレス入力となる乱数Ａ２と、第２の記憶装置３６へのデータ入力となる乱数Ｄ２とを交互に生成する。

【００９９】第１の記憶装置３４および第２の記憶装置３６の構成は、先の実施形態で図３を参照しながら説明した記憶装置２４と同様である。非線形コンバイナ３８の機能は、例えば、２入力１出力の非線形関数ｆである。非線形コンバイナ３８としては、公知のものを使用することができる（例えば文献１参照）。

【０１００】また、非線形コンバイナ３８は、２つの入力データの各ビットの値をもとにした組み合わせ回路で実現しても良い。なお、線形フィードバックシフトレジスタの初期状態や、記憶装置のアドレス入力となる乱数と該乱数により示されるアドレスとの関係についても、先に説明したものと同様である。

【０１０１】次に、図１１を参照しながら本乱数生成装置の動作について説明する。まず、初期処理として、第

１の線形フィードバックシフトレジスタ２０および第２の線形フィードバックシフトレジスタ２２夫々を所望の初期状態にセットする（ステップＳ１１）。

【０１０２】そして、第１の線形フィードバックシフトレジスタ３０により所定ビットの乱数を所定個数生成し、これらを第１の記憶装置３４に格納するとともに、第２の線形フィードバックシフトレジスタ３２により所定ビットの乱数を所定個数生成し、これらを第２の記憶装置３６に格納する（ステップＳ１２）。

【０１０３】次に、第１の線形フィードバックシフトレジスタ３０によりアドレス用の乱数Ａ１を１つ生成するとともに、第２の線形フィードバックシフトレジスタ３２によりアドレス用の乱数Ａ２を１つ生成する。（ステップＳ１３）。

【０１０４】そして、第１の記憶装置３４のアドレスのうち、ステップＳ１３で生成された乱数Ａ２にて示されるアドレスの内容を出力するとともに、第２の記憶装置３６のアドレスのうち、ステップＳ１３で生成された乱数Ａ１にて示されるアドレスの内容を出力する（ステップＳ１４）。

【０１０５】さらに、非線形コンバイナ３８により、ステップＳ１４にて第１の記憶装置３４および第２の記憶装置３６夫々から出力されたデータをもとにした所定の被線形変換処理を実行して、得られたデータを出力する（ステップＳ１５）。

【０１０６】この時点で、生成すべき乱数系列のうち最初の所定ビット分のデータが得られたことになる。次に、第１の線形フィードバックシフトレジスタ３０によりデータ用の乱数Ｄ１を１つ生成するとともに、第２の線形フィードバックシフトレジスタ３２によりデータ用の乱数Ｄ２を１つ生成する（ステップＳ１７）。

【０１０７】そして、第１の記憶装置３４のアドレスのうち、ステップＳ１４で内容の出力されたアドレスに、ステップＳ１７で生成された乱数Ｄ１を格納するとともに、第２の記憶装置３６のアドレスのうち、ステップＳ１４で内容の出力されたアドレスに、ステップＳ１７で生成された乱数Ｄ２を格納する（ステップＳ１８）。

【０１０８】次に、ステップＳ１３に戻って上記と同様に乱数Ａ１とＡ２を生成し（ステップＳ１３）、各記憶装置２４，２６において乱数Ａ２，Ａ１にて示されるアドレスの内容を夫々出力し（ステップＳ１４）、この２つの出力をもとにした所定の被線形変換処理により得られたデータを出力する（ステップＳ１５）。

【０１０９】この時点で、生成すべき乱数系列のうち２番目の所定ビットのデータが得られたことになる。以降、ステップＳ１７，Ｓ１８，Ｓ１３，Ｓ１４，Ｓ１５の処理ループを１回繰り返すごとに、順次、所定ビットの乱数が生成されていく。

【０１１０】そして、ステップＳ１５で必要な長さの乱数系列が得られた場合に、ステップＳ１６でループを抜けて、処理を終了する。なお、本乱数生成装置は、図２を用いて説明した暗号装置および復号装置における乱数系列（鍵系列）を生成するための乱数生成装置として用いると効果的である。この場合、線形フィードバックシフトレジスタ３０の初期状態および線形フィードバックシフトレジスタ３２の初期状態の組そのものまたはこれらを特定可能な識別子が共通鍵として用いられる。

【０１１１】このような本実施形態によれば、記憶装置を緩衝域として用いることで、装置規模に比して線形複雑度が大きく、暗号的にも安全な乱数生成装置、あるいはこれを有する加算型ストリーム暗号の暗号装置および復号装置を実現することができる。

【０１１２】また、装置規模に比して線形複雑度が大きいことは、安価に安全な暗号装置および復号装置を構築できることを意味する。ここで、本実施形態の第１および第２の線形フィードバックシフトレジスタのレジスタ長を各々ＬＡ，ＬＢとすると、本乱数生成装置での線形複雑度は、ほぼ

$2^{LA} \times 2^{LB}$

である。

【０１１３】なお、乱数生成装置のさらに他の構成例として、第１の線形フィードバックシフトレジスタ３０と第２の線形フィードバックシフトレジスタ３２とを１つの線形フィードバックシフトレジスタとして共通化しても良い。

【０１１４】あるいは、その逆に、第１の線形フィードバックシフトレジスタ３０および第２の線形フィードバックシフトレジスタ３２の少なくとも一方を、データ用とアドレス用に分離し、装置全体として３つあるいは４つの線形フィードバックシフトレジスタを設けた構成にすることも可能でる。

【０１１５】また、上記した線形フィードバックシフトレジスタを１、２、３、または４個備えた構成において、少なくとも１つの線形フィードバックシフトレジスタを、他の公知の乱数生成装置（例えば、複数の線形フィードバックシフトレジスタの出力を非線形コンバイナで結合するもの、線形フィードバックシフトレジスタの出力に非線形変換を施すもの、あるいは加算ジェネレータ（ｓｕｍｍａｔｉｏｎｇｅｎｅｒａｔｏｒ）など）に置き換えた構成も考えられる。これを図２の暗号装置および復号装置に適用する場合にも、もちろん、置き換えた乱数生成装置の初期状態そのものまたはこれを特定可能な識別子が共通鍵として用いられる。

【０１１６】図１２に、本発明のさらに他の実施形態に係る乱数生成装置の構成を示す。また、図１１に、本乱数生成装置の動作の流れを示す。本実施形態は、図３の線形フィードバックシフトレジスタの部分を、図３の乱数生成装置自体で置き換えて、構成を階層化したものである。

【０１１７】図１２の他にも、図１０の線形フィードバ

ックシフトレジスタの部分を、図１０の乱数生成装置自体で置き換えた構成も考えられる。あるいは、図３の線形フィードバックシフトレジスタの部分を、図１０の乱数生成装置自体で置き換えた構成や、図１０の線形フィードバックシフトレジスタの部分を、図３の乱数生成装置自体で置き換えた構成も考えられる。

【０１１８】その他、種々の構成が考えられる。また、図１２ように２階層の構造にとどまらず、３階層以上に階層化した乱数生成装置、例えば図１２における線形フィードバックシフトレジスタの部分を、さらに図３の乱数生成装置あるいは図１２の乱数生成装置で置き換えた構成など、種々のものが考えられる。

【０１１９】また、以上の各機能は、ソフトウェアとしても実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１２０】

【発明の効果】本発明に係る乱数生成装置や方法によれば、記憶装置を緩衝域として用いることで、少ない装置規模で大きな線形複雑度を達成することができる。従って、本発明に係る乱数生成装置や方法を適用することにより、経済的かつ安全なストリーム暗号を実現することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る乱数生成装置の構成を示す図

【図２】本発明の実施の形態に係る乱数生成装置を用いた暗号システムの一例を示す図

【図３】本発明の一実施形態に係る乱数生成装置の構成を示す図

【図４】同実施形態に係る乱数生成装置の動作を示すフローチャート

【図５】生成されたアドレス系列を示す図

【図６】記憶装置の内容の遷移を示す図

【図７】記憶装置の内容の遷移を示す図

【図８】変換前後の乱数系列を示す図

【図９】同実施形態に係る乱数生成装置の変形例の構成を示す図

【図１０】本発明の他の実施形態に係る乱数生成装置の構成を示す図

【図１１】同実施形態に係る乱数生成装置の動作を示すフローチャート

【図１２】本発明のさらに他の実施形態に係る乱数生成装置の構成を示す図

【図１３】線形フィードバックシフトレジスタの構成例を示す図

【図１４】他の乱数生成装置の構成例を示す図

【符号の説明】

２，４，４０，４２…乱数生成部

６…乱数変換部

１０ａ，１０ｂ…乱数生成装置

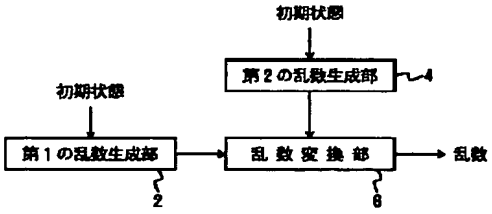
１２ａ，１２ｂ…論理演算処理装置

２０，２２，２６，３０，３２…線形フィードバックシフトレジスタ

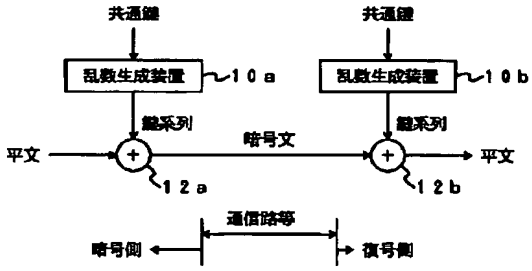
２４，３４，３６…記憶装置

３８…非線形コンバイナ

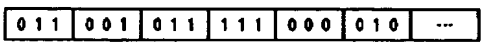
【図１】



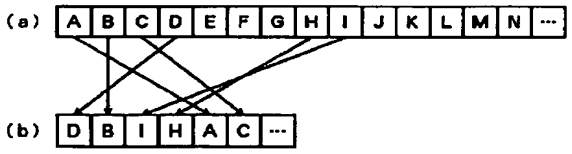

【図２】



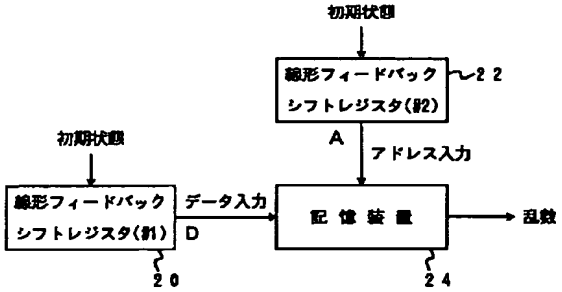

【図５】




【図８】



【図3】




【図6】

| アドレス | 内容 |
|---|---|
| 000 | |
| 001 | |
| 010 | |
| 011 | |
| 100 | |
| 101 | |
| 110 | |
| 111 | |

(a)

| アドレス | 内容 |
|---|---|
| 000 | A |
| 001 | B |
| 010 | C |
| 011 | D |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(b)

| アドレス | 内容 |
|---|---|
| 000 | A |
| 001 | B |
| 010 | C |
| 011 | I |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(c)

| アドレス | 内容 |
|---|---|
| 000 | A |
| 001 | J |
| 010 | C |
| 011 | I |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(d)

【図7】

| アドレス | 内容 |
|---|---|
| 000 | A |
| 001 | J |
| 010 | C |
| 011 | K |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(a)

| アドレス | 内容 |
|---|---|
| 000 | A |
| 001 | J |
| 010 | C |
| 011 | K |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | L |

(b)

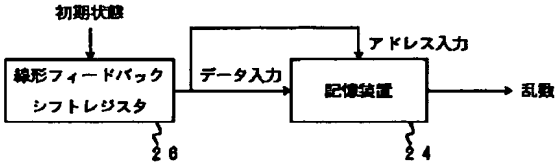
| アドレス | 内容 |
|---|---|
| 000 | M |
| 001 | J |
| 010 | C |
| 011 | K |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | L |

(c)

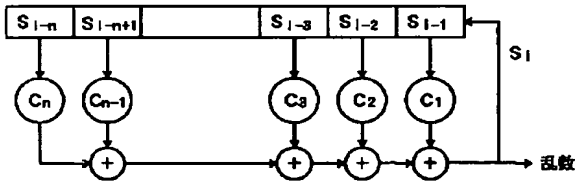
| アドレス | 内容 |
|---|---|
| 000 | M |
| 001 | B |
| 010 | N |
| 011 | D |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(d)

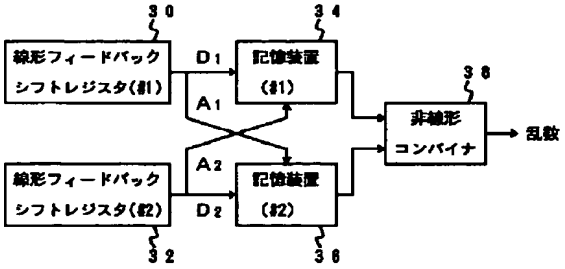
【図9】



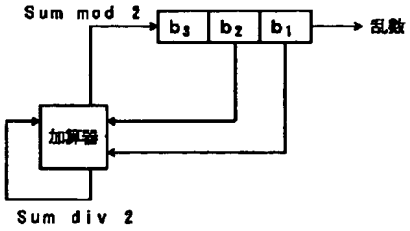

【図13】



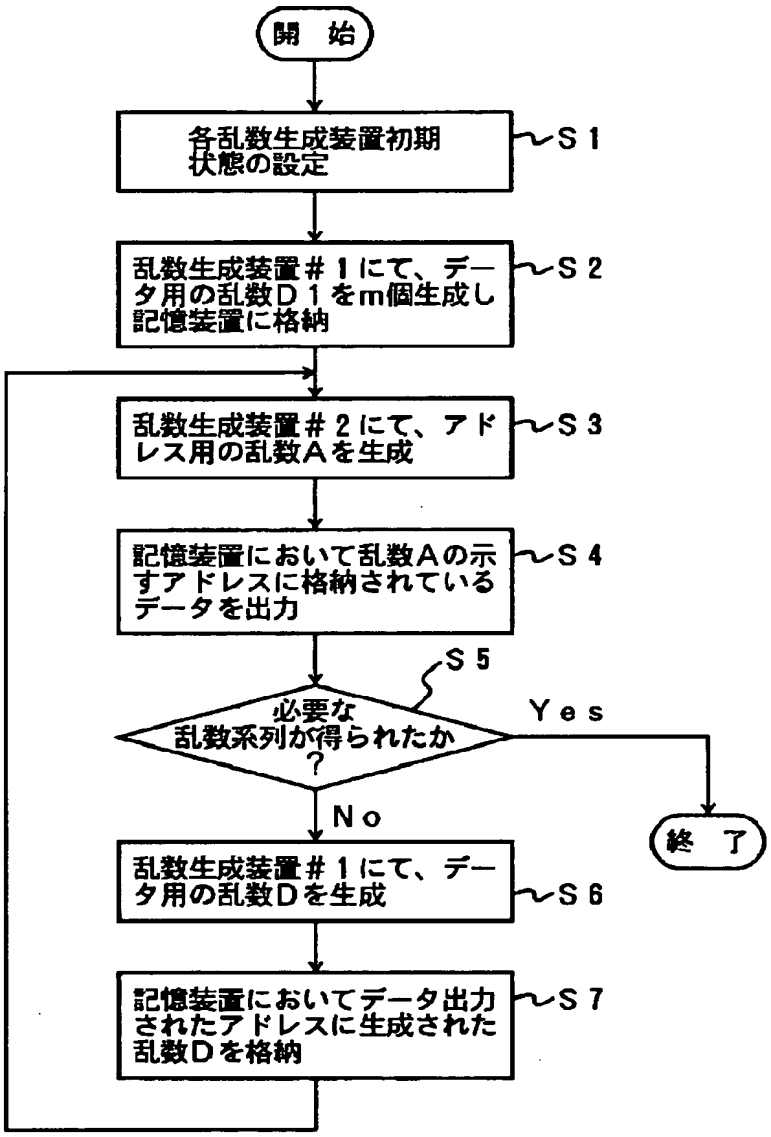

【図10】



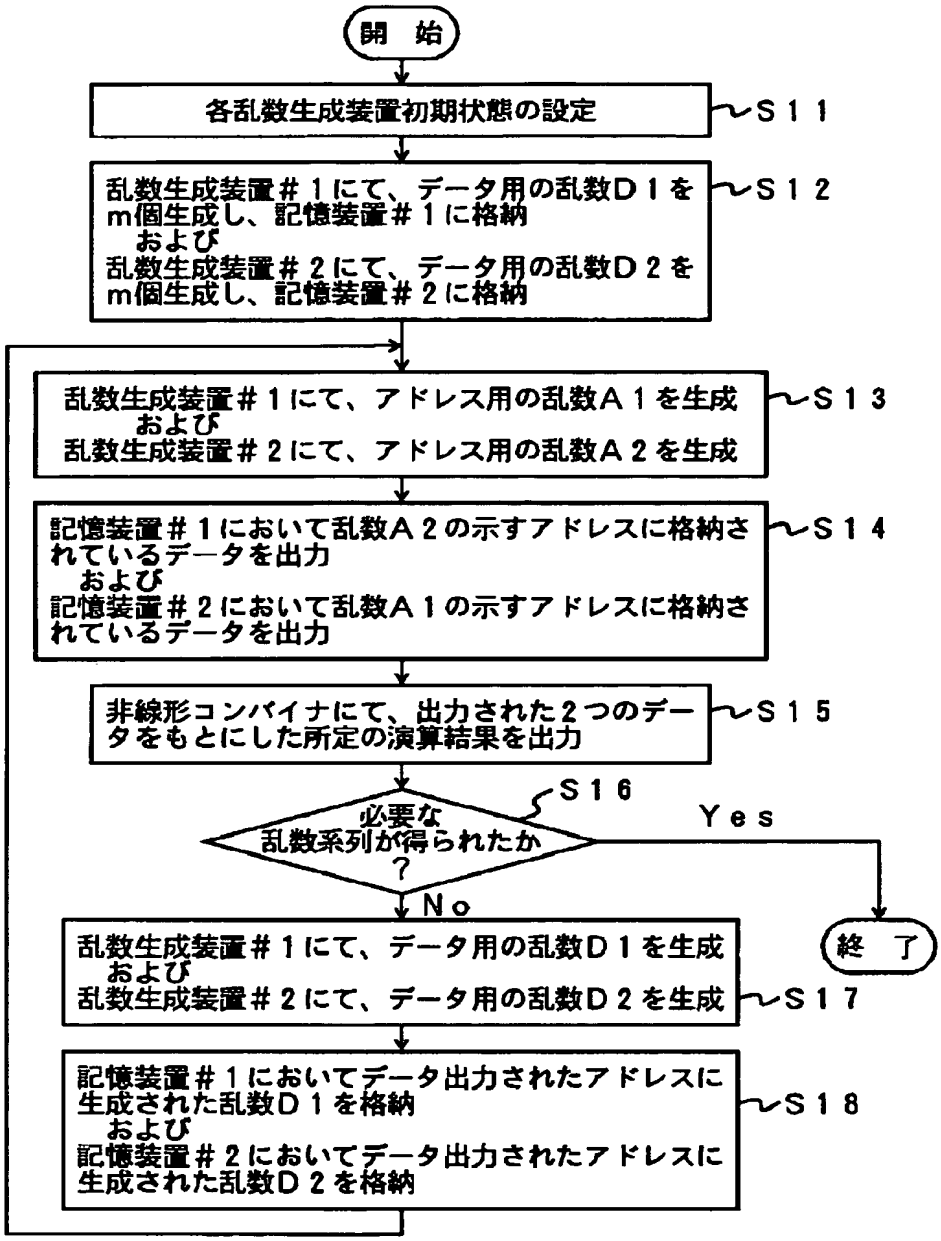

【図14】



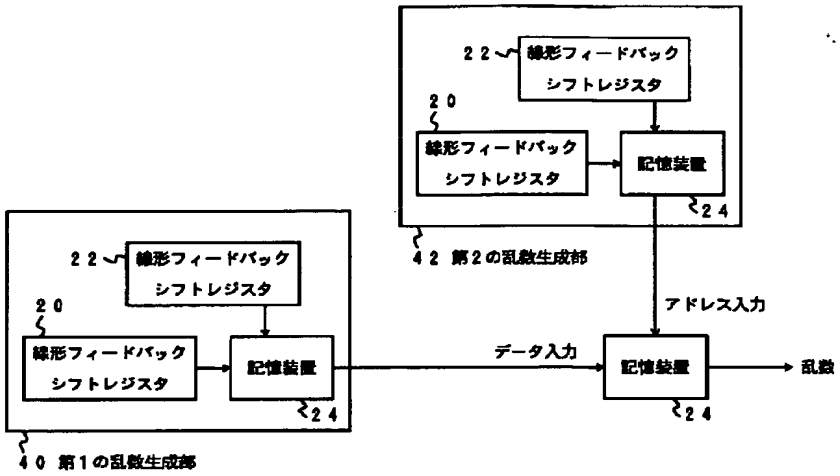
【図4】



【図11】


開　始
各乱数生成装置初期状態の設定
S11
乱数生成装置＃1にて、データ用の乱数D1をm個生成し、記憶装置＃1に格納
および
乱数生成装置＃2にて、データ用の乱数D2をm個生成し、記憶装置＃2に格納
S12
乱数生成装置＃1にて、アドレス用の乱数A1を生成
および
乱数生成装置＃2にて、アドレス用の乱数A2を生成
S13
記憶装置＃1において乱数A2の示すアドレスに格納されているデータを出力
および
記憶装置＃2において乱数A1の示すアドレスに格納されているデータを出力
S14
非線形コンバイナにて、出力された2つのデータをもとにした所定の演算結果を出力
S15
必要な乱数系列が得られたか？
S16
Yes
No
終　了
乱数生成装置＃1にて、データ用の乱数D1を生成
および
乱数生成装置＃2にて、データ用の乱数D2を生成
S17
記憶装置＃1においてデータ出力されたアドレスに生成された乱数D1を格納
および
記憶装置＃2においてデータ出力されたアドレスに生成された乱数D2を格納
S18

【図12】


22 線形フィードバック
シフトレジスタ
20
線形フィードバック
シフトレジスタ
記憶装置
24
42 第2の乱数生成部
アドレス入力
22 線形フィードバック
シフトレジスタ
20
線形フィードバック
シフトレジスタ
記憶装置
24
データ入力
記憶装置
24
乱数
40 第1の乱数生成部